

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-248031

(43)Date of publication of application : 06.11.1991

(51)Int.Cl.

G01M 3/20

(21)Application number : 02-044447

(71)Applicant : MITSUBISHI HEAVY IND LTD

(22)Date of filing : 27.02.1990

(72)Inventor : KINOMOTO TOSHIAKI
YOSHIDA YASUYUKI

(54) METHOD FOR SPECIFYING LEAKING PART

(57)Abstract:

PURPOSE: To confirm the presence or absence of leaking material by making sodium nitrite in mixture leaked from the leaking part of a heat medium react with p,p'-diaminodiphenyl methanesulfonic hydrochloride, and detecting the presence of generated blue coloring matter.

CONSTITUTION: A small amount of heat medium leaks through a pin hole or a crack which is formed at the welded part of the pipe and the pipe plate and the like in a heat exchanger. With the nitrite in this heat medium, 1% aqueous solution of hydrochloric acid of 1% p,p'-diaminodiphenyl methanesulfonic hydrochloride is made to react. Thus blue coloring matter is generated, and the leaking part can be specified simply. At this time, the reagent is synthesized by sulfonating 4,4'-diaminodiphenyl methane with fuming sulfuric acid, adding barium chloride and removing sulfuric acid radical, eventually synthesized as an aqueous solution of hydrochloric acid. The nitrous-acid detecting sensitivity of the 1% aqueous solution of hydrochloric acid of the 1% p,p'-diaminodiphenyl methanesulfonic hydrochloride is very high, and the presence of nitrous acid can be sufficiently confirmed even with 0.3 μ g-NO₂-.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

⑫ 公開特許公報(A)

平2-44447

⑬ Int.Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)2月14日

G 06 F 12/14
B 41 J 5/30
29/00
29/13
29/38
29/46
G 06 F 1/16
G 06 K 19/073

3 2 0 D 7737-5B
Z 7810-2C

Z 8804-2C
Z 8804-2C

6711-5B G 06 K 19/00 P
8804-2C B 41 J 29/00 U
8804-2C 29/12 C
7459-5B G 06 F 1/00 3 1 3 C

審査請求 未請求 請求項の数 5 (全10頁)

⑮ 発明の名称 攻撃対抗容器

⑯ 特 願 昭63-195847

⑰ 出 願 昭63(1988)8月5日

⑱ 発 明 者 森 亮 一 東京都文京区白山1-24-12

⑲ 出 願 人 森 亮 一 東京都文京区白山1-24-12

⑳ 代 理 人 弁理士 山田 武樹

明 細 書

1. 発明の名称

攻撃対抗容器

2. 特許請求の範囲

(1) 内部に秘密情報を収納した容器の外周面に論理素子を並べ、該論理素子が正常動作を失うことをもって外部からの攻撃の検出を行うことを特徴とする攻撃対抗容器。

(2) 前記論理素子が、メモリー素子を構成することを特徴とする特許請求の範囲第1項記載の攻撃対抗容器。

(3) 前記論理素子が、前記容器の全外周面に設けられていることを特徴とする特許請求の範囲第1項記載の攻撃対抗容器。

(4) 前記論理素子が、前記容器の外周面の一部に設けられていることを特徴とする特許請求の範囲第1項記載の攻撃対抗容器。

(5) 前記論理素子が、前記容器の外周面に複数の層をなして設けられていることを特徴とする特許請求の範囲第1項記載の攻撃対抗容器。

3. 発明の詳細な説明

(1) 産業上の利用分野

本発明は、内部に収納した秘密情報を解読しようとする攻撃に対抗するようにした攻撃対抗容器に関する。

(2) 従来の技術

電子計算機システムのセキュリティーを信頼できるものとするためには、システムのある部分への物理的アクセスをユーザーに許可しない機構が必要となってくる。これは、例えばこの部分の内容についてユーザーがコピーをとることやコードを変更すること等を制限する場合に特に必要となってくる。

このような場合に、秘密にしておきたいシステムのある部分を容器に収め、この容器に対して内部の秘密情報を解読しようとする攻撃、例えば容器に穴を開ける行為があったときには、内部の秘密情報を消去することで攻撃に対抗することが行われる。このようにして攻撃に対抗する容器は、攻撃対抗容器(Tamper Resistant Module)と呼

ばれている。

従来の攻撃対抗容器として、Steve H. Weingart (IBM Thomas J. Watson Research Center) の「Physical Security for the μ ABYSS System (Proceedings, 1987 IEEE Symposium on Security and Privacy, Oakland, CA, April 27-29, 1987, pp.55-58)」が知られている。

これは、秘密情報を内部に収納した容器の周囲を細いワイヤー（ニクロム線）で巻装し、ワイヤーが切られたり、短絡したり、接続を変えようとしたときには、その抵抗値が変化することから攻撃を検出して内部の秘密情報を消去するものであった。

(3) 発明が解決しようとする課題

しかしながら、細いワイヤーで容器を多層に巻装する工程は量産に適さず、また、ワイヤーの抵抗値が経時変化や温度等の環境変化によって変るために、存在しない攻撃を誤って検出して内部の秘密情報を消去してしまうという問題点があった。

第1図は、本発明による攻撃対抗容器の一実施例を示す斜視図である。また、第2図は、本発明による攻撃対抗容器の一実施例を示す分解平面図である。

第1図において、攻撃対抗容器1は2枚の基板2および3によって構成され、基板2および3は、第2図に示すように、基板2の接合部2aと基板3の接合部3aとを接合することによって形成される。接合部2aおよび接合部3aにもメモリー素子4は存在し、接合はメモリー素子4に直接行われるか、またはメモリー素子4に堅固に継がれた層を介して行われる。接合強度は、第6図で説明するトランジスタ8の各構成層の分離に対する強度よりも大きくなるように接着面積の設定や接着剤の選択が行われる。なお、強度とは、攻撃に対する強度である。

このような接合によって作られる攻撃対抗容器1は、極めて薄くできるので、側面方向からの攻撃に対して上下面方向と同じ検出精度を持っている。攻撃対抗容器1が厚くなる場合には、攻撃対

また、実在する攻撃を看過して、内部の秘密情報を消去すべきときに消去を失敗するという問題があった。

(4) 課題を解決するための手段

本発明は、上記の点に鑑みてなされたもので、量産が可能でありかつ誤って攻撃を検出して内部の秘密情報を消去してしまうことがないようにすることを目的とし、この目的を達成するために、内部に秘密情報を収納した容器の外周面に論理素子を並べ、論理素子が正常動作を失うことをもって外部からの攻撃の検出を行うように構成されている。

(5) 作用

この構成において、容器の外周面に論理素子を並べるようにしたことで、量産が可能となり、また、論理素子の動作を検出して外部からの攻撃の検出を行うことで、誤って攻撃を検出することがないようにしている。

(6) 実施例

以下、本発明を図面に基づいて説明する。

抗容器1の側面にもメモリー素子4を配置することによって他の上下面と同様な検出精度を維持できる。

秘密情報は、メモリー素子等の形態で接合部2aと接合部3aとの接合面の内側に置かれる。接合部2aと接合部3aは、それぞれ基板2および基板3の片面周辺部に接着剤を塗布することによって形成される。なお、攻撃対抗容器1の大きさは、一辺が数mmから数十cm程度であるが、後述するメモリー素子4の大きさによる下限はあるものの、上限は事実上制約がない。

基板2の上面（第1図）および基板3の下面には、第3図に示すメモリー素子4が気相法等によって形成される。第3図に示すメモリー素子4は、3個のトランジスタTr1、Tr2、Tr3でダイナミックメモリーを構成した場合の例であり、J. Newkirk and R. Mathews の「The VLSI Designer's Library」(Addison-Wisley, 1983) で開示されている。メモリー素子4は、ダイナミック

メモリーに限ることなく、スタティックメモリーで構成することも可能である。メモリー素子4は、基板2および基板3の表面に複数個並べて配置され、それぞれのメモリー素子4の書き込みクロック線、読み出しクロック線、データ線、接地線は、互に接続されている。なお、第1図では、メモリー素子4の配列の一部分のみを拡大して記載してある。個々のトランジスタ T_{r1} 、 T_{r2} 、 T_{r3} の大きさは数十 μm である。また、図面の記載を明確にするために、第3図(a)に示すメモリー素子4を、以下では第3図(b)のように模式化して表現するものとする。

メモリー素子4は、基板2および基板3の表面に第4図または第5図に示すように配置される。すなわち、トランジスタ T_{r1} 、 T_{r2} 、 T_{r3} が市松模様を成すように構成される。第4図(a)のA-A線断面図は第4図(b)のようになる。

基板2および基板3の表面に配置されたトランジスタ T_{r1} 、 T_{r2} 、 T_{r3} のうちの一個でも攻撃が行われた場合には、メモリー素子4がメモリー

素子としての機能を失うので、第20図で後述する回路によってメモリー素子4の記憶内容を繰返し読み出すことでメモリー素子としての機能を検出し、メモリー素子としての機能を失ったメモリー素子4が検出されたときには、攻撃を受けたものとして内部の秘密情報を消去するようにしている。なお、本明細書中で攻撃とは、機械力、温度変化、化学薬品、生化学手段、レーザー等によって、内部の秘密情報を解読しようとする行為を言うものとする。

この第4図に示す例では、トランジスタ T_{r1} 、 T_{r2} 、 T_{r3} の大きさを ϵ とし、トランジスタ T_{r1} 、 T_{r2} 、 T_{r3} はその一部が欠損しても機能するものとする、最悪の場合には開口5で示す一辺が約3 ϵ の穴を開けるまでは、攻撃を検出できない場合が出てくる。

そこで、第5図に示す例では、メモリー素子4による第1層6と第2層7との2層を重ねるようにしている。すなわち、第5図(a)のA-A線断面図は第5図(c)になるように、また、第5

図(b)のB-B線断面図は第5図(d)になるようにして、第1層6と第2層7との2層を重ねるようにしている。これにより、第1層6と第2層7を外側からみると、トランジスタ T_{r1} 、 T_{r2} 、 T_{r3} のいずれかのトランジスタで覆われることになるので、最悪の場合でも一辺が約2 ϵ の穴を開けるだけで攻撃を検出できるようになる。

この考えを進めて、更に多層化を図ることで攻撃検出できる穴の直径を限りなく ϵ にまで近づけることができる。また、メモリー素子4のメモリー素子としての機能を検出する際に、多層化した各層間で論理積や論理和をとることで攻撃検出の感度を調節することができ、メモリー素子4の一時的エラーや恒久的エラーによる誤検出を避けることができる。また、逆に秘密情報が存在する部分に応じて外周面の一部分にのみメモリー素子4を設けて、エラーによる誤検出を避けるようにもできる。

以上で述べた第1図～第5図に示す攻撃対抗容器では、メモリー素子4を構成する小さなMOS

トランジスタ T_{r1} 、 T_{r2} 、 T_{r3} を多数個配置する実施例について説明したが、個々のトランジスタ T_{r1} 、 T_{r2} 、 T_{r3} について、ある一方向を大きくすることも可能である。第6図(a)は、このように一方向の寸法を大きくしたMOSトランジスタ8の例を示している。

第6図(a)において、トランジスタ8は3層のソース8a、ゲート8b、ドレイン8cによって構成され、ソース8aおよびドレイン8cのリード線は図面の右側に引出され、ゲート8bのリード線は図面の左側に引出されている。トランジスタ8は、基板2の上面および基板3の下面(共に第1図)に気相法等によって形成される。ソース8aおよびドレイン8cのいずれかを攻撃対抗容器1の外側にするかは任意である。

第6図(b)および(c)は、ソース8aが攻撃対抗容器1の外側にあって、機械的な攻撃を受けた場合を示している。第6図(b)は、ソース8aおよびゲート8bまで機械的な攻撃を受けた場合を示しており、トランジスタ8の3層のうち

の2層を左右(第6図)に分断する攻撃があったときには、トランジスタ8はトランジスタとしての機能を失い、このトランジスタ8によって構成されるメモリー素子が機能を失ったことが検出されたときには、攻撃を受けたものとして内部の秘密情報を消去するようにしている。

第6図(c)は、ソース8a、ゲート8b、ドレイン8cの3層が機械的な攻撃を受けた場合を示しており、トランジスタ8の3層の全部が左右(第6図)に分断されるので、トランジスタ8はトランジスタとしての機能を失い、上述した第6図(b)に示す場合と同様に、攻撃を受けたものとして内部の秘密情報を消去するようにしている。

第7図は、第6図では直線状であったトランジスタ8をジグザグ状に形成した場合を示す平面図である。ソース8aおよびドレイン8cのリード線は図面の左下側に引出され、ゲート8bのリード線は図面の左上側に引出されている。トランジスタ8は、基板2の上面および基板3の下面(共に第1図)に気相法等によって形成され

る。第7図に示すトランジスタ8は、一個当たりの面積が広いので、基板2または基板3上に形成する個数を低減することができる。

第8図は、第7図で示したトランジスタ8をジグザグ状に形成した場合の変形例を示す平面図である。ソース8a、ドレイン8c、ドレイン8cの全てのリード線は図面の左上側に引出されるので、配線が容易になる場合がある。また、バイファイラー巻きになっているので、往路と復路における誘導信号を相殺することができ、ノイズマージンを高く設定できる。

第9図は、第6図では直線状であったトランジスタ8を渦巻き状に形成した場合を示す平面図である。ソース8aおよびドレイン8cのリード線は中心部から引出され、ゲート8bのリード線は外周部から引出されている。第9図に示すトランジスタ8は、一個当たりの面積が広いので、基板2または基板3上に形成する個数を低減することができる。

第10図は、第9図で示したトランジスタ8を

渦巻き状に形成した場合の変形例を示す平面図である。ソース8a、ドレイン8c、ドレイン8cの全てのリード線は外周部から引出されるので、配線が容易になる。また、バイファイラー巻きになっているので、往路と復路における誘導信号を相殺することができ、ノイズマージンを高く設定できる。

第11図は、第1図で示した攻撃対抗容器1の変形例を示す斜視図である。図中、第1図と同じ構成部分には同じ参照番号を付して重複した説明を省略する。

第11図に示す攻撃対抗容器1は、基板2と基板3が第12図に示すように1枚の基板で作成され、第12図の破線の部分を折り曲げることで基板2と基板3の接合が行われる。接合強度は、第6図で説明したトランジスタ8の各構成層の分離に対する強度よりも大きくなるように接着面積の設定や接着剤の選択が行われる。なお、強度とは、攻撃に対する強度である。

第13図は、第12図の破線の部分を折り曲げ

ることで基板2と基板3の接合を行った場合に、折り曲げ部と接合部とで強度に差異が生ずるので、折り曲げ部の位置が4方向に分散するように、基板2と基板3の組合せを4層にした場合を示している。すなわち、最も内周の基板2と基板3の組合せは、折り曲げ部の位置が第13図の上方向にある。次の基板2と基板3の組合せは、折り曲げ部の位置が第13図の右方向にあり、更に次の基板2と基板3の組合せは、折り曲げ部の位置が第13図の左方向にあり、最も外周の基板2と基板3の組合せは、折り曲げ部の位置が第13図の下方向にある。

このように、折り曲げ部の位置を分散したことで、4方向のいずれの方向からの攻撃に対する強度も均一にできる。

第14図は、第1図で示した攻撃対抗容器1の他の変形例を示す斜視図である。図中、第1図または第11図～第13図と同じ構成部分には同じ参照番号を付して重複した説明を省略する。

第14図に示す攻撃対抗容器1は、基板2と基

板3が第15図に示すように1枚の基板で作成され、第12図の破線の部分を折り曲げることで基板2と基板3の接合が行われる。このとき、基板2の一部と基板3の一部が攻撃対抗容器1の中央部で重なるようにして折り曲げられる。

第16図は、基板2の一部と基板3の一部が攻撃対抗容器1の中央部で重なるようにして折り曲げた場合に、中央部で重なった部分の強度が他の部分と異なるので、重なった部分の位置が2方向に交差するように、基板2と基板3の組合せを2層にした場合を示している。すなわち、内周の基板2と基板3の組合せは、重なった部分の位置が第16図の横方向にある。外周の基板2と基板3の組合せは、重なった部分の位置が第16図の縦方向にある。

このように、重なった部分の位置が交差するようにしたこと、縦横のいずれの方向からの攻撃に対する強度も均一にできる。

第17図から第19図は、第1図で示した攻撃対抗容器1の他の変形例を示す斜視図である。図

中、第1図または第11図～第16図と同じ構成部分には同じ参照番号を付して重複した説明を省略する。

第17図に示す攻撃対抗容器1は、基板2と基板3が1枚の長方形基板で作成され、第12図の破線の部分を3箇所折り曲げることで接合部2aと接合部3aの部分で接合が行われる。

第18図は、接合部2aと接合部3aの部分の位置が異なる3種類の攻撃対抗容器1を用意することを意味している。これらの3種類の攻撃対抗容器1は、第19図に示すように立方体状に組合せられる。このように、立方体状に攻撃対抗容器1を構成することで、攻撃対抗容器1の内部には立体物の秘密情報を置くことができる。

第20図は、攻撃を検出して対抗するために秘密情報を消去する回路を示している。秘密情報は、RAMメモリー素子で構成される秘密保持回路14に書き込まれている。この秘密保持回路14を含めて、アドレス発生回路10、読み出し結果判定回路11、秘密消去回路12、書き込み回路17、

読出し回路18が攻撃対抗容器1の内側に置かれ、メモリー素子4が、攻撃対抗容器1の外側に置かれる。電源13は、攻撃対抗容器1の内側に置かれてもよく、また後にバックアップおよび瞬断に関して説明する構成をとれば、攻撃対抗容器1の外側に置いてもよい。

第20図では、メモリー素子4がダイナミックRAMによって構成される場合を示している。メモリー素子4には、アドレス発生回路10からアドレス信号が供給されており、指定されたアドレスのメモリー素子4に、書き込み回路17がランダムな値あるいは所定の値のビットを書込む。アドレス発生回路10は、例えばカウンタによって構成され、全てのメモリー素子4を漏れなくアドレス指定する。このようにアドレスが指定されて、値が書込まれたメモリー素子4の内容は、読出し回路18によって直ちに読出される。従ってメモリー素子4は、ダイナミックRAMによって構成されているが、リフレッシュ動作は必要としない。

メモリー素子4に書込まれた値とメモリー素子4から読み出された値は読み出し結果判定回路11に供給される。読み出し結果判定回路11は、例えば排他的論理和回路によって構成され、メモリー素子4に書込まれた値とメモリー素子4から読み出された値が一致するかどうかを検査する。

次に、同じアドレスのメモリー素子4に対して書込む値、すなわち0と1とを反転して、メモリー素子4に書込まれた値とメモリー素子4から読み出された値が一致するかどうかを再度検査する。これにより、メモリー素子4を構成する全てのトランジスタTr1、Tr2、Tr3の機能を必要十分に検査できる。

検査結果は秘密消去回路12に供給される。

秘密消去回路12は、例えば電源13からの配線を抵抗19を介して接地するアナログスイッチによって構成され、通常はオフ状態になっている。秘密消去回路12がオフ状態になっていることで、電源13の電力が秘密保持回路14に供給され、RAMメモリー素子で構成される秘密保持回路1

4に書き込まれている秘密情報が保持される。秘密保持回路14に書き込まれている秘密情報は、入力端子15を介して書込まれ、また出力端子16を介して読み出しが行われている。読み出した信号は、攻撃対抗容器1内だけで利用することができる。

攻撃対抗容器1に対する攻撃があったときには、上述のごとくメモリー素子4を構成するトランジスタTr1、Tr2、Tr3のいずれかが破壊されるので、メモリー素子4は、メモリー素子としての機能を失い、書込まれた内容を正しく出力することができなくなる。

メモリー素子4の書込み・読み出し内容に不一致があると、読み出し結果判定回路11はこれを検出して秘密消去回路12をオン状態にする。秘密消去回路12がオン状態になることで、秘密保持回路14は電力の供給が断たれて、その記憶内容を消去する。

なお、電源13およびメモリー素子4、アドレス発生回路10、読み出し結果判定回路11、秘

密消去回路12、書込み回路17、読み出し回路18の電源は、攻撃対抗容器1に内蔵された電池である必要はなく、外部の商用電源から供給される電源と、この商用電源が切られているときにバックアップするための外部または内蔵の電池とで構成することができる。また、電源の電池が外付けである場合に、電池交換等のためにこの電池を取外しているときの、外部の商用電源の瞬断に対応するための外付けまたは内蔵の大容量のコンデンサーとで構成することもできる。

電源13等をこのように構成した場合において、電源切れが起きたとき、すなわち、バックアップ電池が取外されているか又は消耗して外部の商用電源が瞬時を越えて停電したときには、メモリー素子4、アドレス発生回路10、読み出し結果判定回路11、秘密消去回路12、書込み回路17、読み出し回路18の電源が、秘密保持回路14の電源よりも後で切れるように動作電圧および時定数等が設定されていれば、秘密保持回路14の記憶内容を保護する目的は達成できる。なぜならば、

秘密保持回路14の記憶内容(秘密情報)が存在する間は、攻撃検出機能および秘密消去機能が働いているからである。

また、極低温では、電源なしでも秘密保持回路14の記憶内容(秘密情報)が維持される場合があるが、その場合には通常の動作温度から極低温に至るまでの時間が十分に長いので、低温になる前に温度に依る攻撃として検出が行われ、秘密保持回路14の記憶内容の抹消が行われる。

第20図で説明した回路は、種々の変形が可能である。例えば、メモリー素子4はRAMではなく、ROMやEPROMで構成することもできる。ただし、メモリー素子4をROMまたはEPROMで構成した場合には、書き込み回路が不要となる。

メモリー素子4の全体の検査が一巡するまでの所用時間は、攻撃を開始して秘密情報を読み始めるまでに必要な時間より短ければ十分である。それは例えば数秒のオーダーであり、メモリー素子4の全部を検

査する速度は、例えばビデオディスプレイメモリーのリフレッシュサイクルよりも遅くてよい。メモリー素子4の数が極めて多い場合には、メモリー素子4の全体を複数のバンクに分割し、各バンクに対応して攻撃を検出する回路を複数個設置することによって、検査速度を向上することもできる。

また、製造上の理由によってあるアドレスに検出素子がないとか、あるアドレスの検出素子が不良であることが判っている場合がある。このような場合には、そのアドレスについての攻撃検出を行わないようにできる。攻撃検出を行わないアドレスが相当数ある場合には、攻撃検出を行わないアドレスを表した不検査ビットマップを用いるようにもできる。この場合には、不検査ビットマップをROMで構成し、製造後出荷前に検出素子がないとか検出素子が不良であるアドレスを調べて、そのROMに書き込むようにできる。

第20図に示す攻撃対抗回路に守られた容器内の装置が、外部と通信を行うようにすることもで

きる。また、アドレス保持レジスタを設けて、読み出し結果判定回路11が攻撃を検出したときのアドレス発生回路10の出力アドレスを記憶しておいて、後日の検査の便宜を図ることもできる。同様にタイム保持レジスタを設けて、読み出し結果判定回路11が攻撃を検出したときのリアルタイムカウンターの出力を記憶しておいて、後日の検査の便宜を図ることもできる。

電源電圧や温度を測定して、低すぎたり高すぎたりしたときに、攻撃があったものと判断するようにもできる。

以上、本発明を実施例により説明したが、本発明の技術的思想によれば、種々の変形が可能である。例えば、上述した実施例では、内部に秘密情報を収納した容器の外周面にメモリー素子を設け、このメモリー素子の記憶内容を検出することで攻撃検出を行うようにしたが、メモリー素子以外のデジタル素子、例えばシフトレジスタや超伝導に依る論理素子等を並べて、その動作が維持されているか否かを検出することで攻撃検出を行うよう

にすることもできる。

(7) 発明の効果

以上で説明したように、本発明は、内部に秘密情報を収納した容器の外周面に論理素子を並べ、論理素子が正常動作を失うことをもって外部からの攻撃の検出を行うように構成されている。この構成により、容器の外周面に論理素子を並べるようにしたことで、量産が可能となり、また、論理素子の動作を検出して外部からの攻撃の検出を行うことで、誤った攻撃検出を排除することが可能となる。

4. 図面の簡単な説明

第1図は、本発明による攻撃対抗容器の一実施例を示す斜視図、

第2図は、本発明による攻撃対抗容器の一実施例を示す平面図、

第3図は、本発明による攻撃対抗容器の一実施例を示すブロック図、

第4図は、本発明による攻撃対抗容器の一実施例を示す平面図と断面図、

第5図は、本発明による攻撃対抗容器の一実施例を示す平面図と断面図、

第6図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第7図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第8図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第9図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第10図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第11図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第12図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第13図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第14図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第15図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第16図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第17図は、本発明による攻撃対抗容器の他の実施例を示す平面図、

第18図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第19図は、本発明による攻撃対抗容器の他の実施例を示す斜視図、

第20図は、本発明による攻撃対抗容器の一実施例を示すブロック図である。

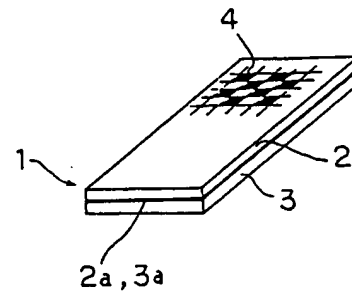
- 1 攻撃対抗容器
- 2 基板
- 3 基板
- 4 メモリー素子
- 5 開口
- 6 第1層
- 7 第2層

- 8 トランジスタ
- 10 アドレス発生回路
- 11 読み出し結果判定回路
- 12 秘密消去回路
- 13 電源
- 14 秘密保持回路
- 15 入力端子
- 16 出力端子
- 17 書き込み回路
- 18 読み出し回路
- 19 抵抗

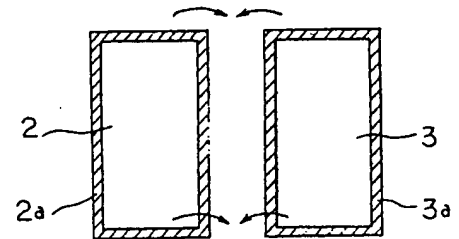
特許出願人 森 亮 一

代理人 弁理士 山 田 武 樹

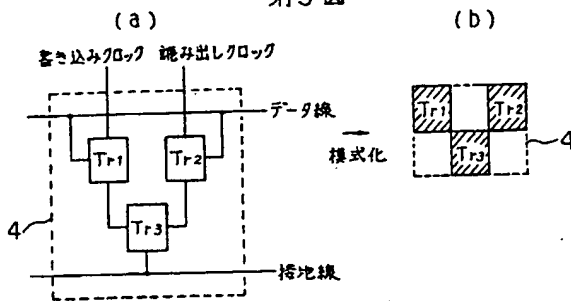
第1図



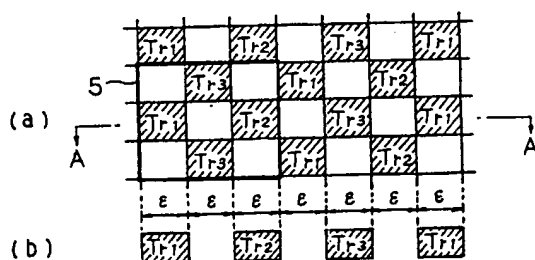
第2図



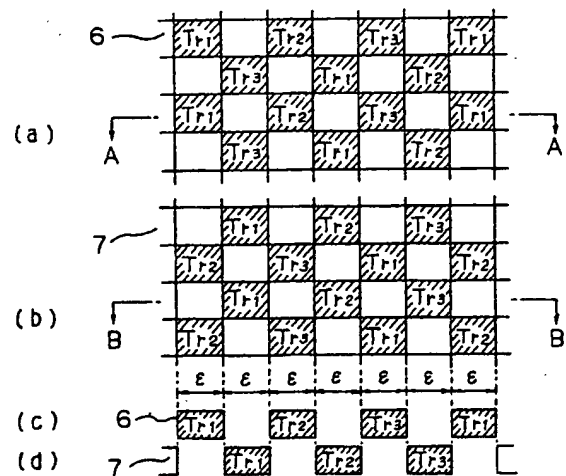
第3図



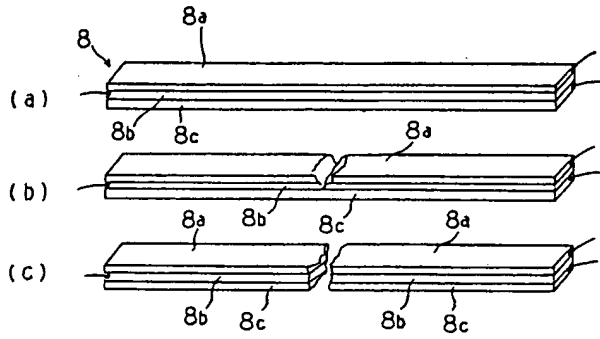
第4図



第5図



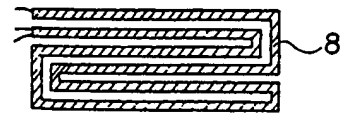
第6図



第7図



第8図



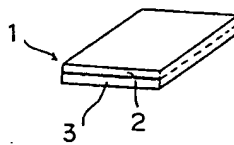
第9図



第10図



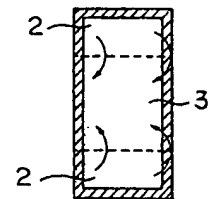
第11図



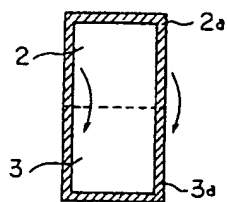
第14図



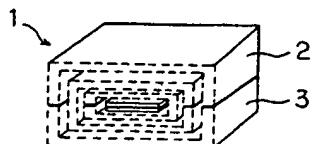
第15図



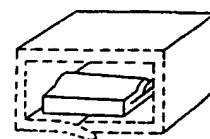
第12図



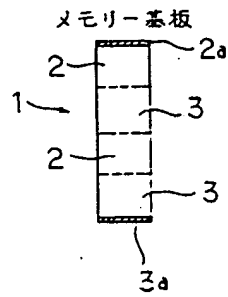
第13図



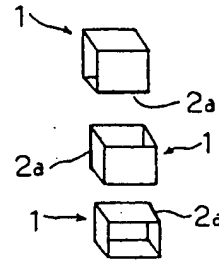
第16図



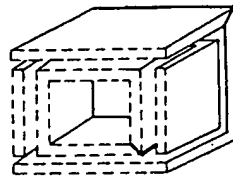
第17図



第18図



第19図



第20図

